PIONEER
ACADEMIC PUBLISHING LIMITED

Studies in Law and Justice
ISSN 2958-0382
www.pioneerpublisher.com/slj
Volume 2 Number 2 June 2023

Research on Criminal Risk Analysis and Governance Mechanism of Generative Artificial Intelligence such as ChatGPT

Yifeng Tong[1]

[1] College of Criminal Law, East China University of Political Science and Law
Correspondence: Yifeng Tong, College of Criminal Law, East China University of Political Science and Law.

doi:10.56397/SLJ.2023.06.13

Abstract

The launch of ChatGPT marks a breakthrough in the development of generative artificial intelligence (generative AI) technology, which is based on the collection and learning of big data as its core operating mechanism. Now the generative AI has the characteristics of high intelligence and high generalization and thus has led to various criminal risks. The current criminal law norms are inadequate in terms of the attribution system and crime norms for the criminal risks caused by the generative AI technologies. Thus, we should clarify the types of risks and governance challenges of generative AI, clarify that data is the object of risk governance, and establish a pluralistic liability allocation mechanism and a mixed legal governance framework of criminal, civil, and administrative law on this basis.

Keywords: ChatGPT, generative artificial intelligence, risk analysis, risk governance

1. Introduction

On November 20, 2022, OpenAI released ChatGPT, an intelligent chat AI bot, which set off a wave of technological revolution in the field of artificial intelligence. As the latest technological achievement of generative artificial intelligence, ChatGPT relies on its powerful algorithm technology to conduct conversations with users like real people, and can even perform highly specialized activities such as writing articles and taking exams. ChatGPT's grassroots technology mechanism is to achieve the current intelligence by imitating the neuronal network of the human brain through computer parameters. There are 100 billion neurons in the human brain, and according to the data provided by OpenAI, ChatGPT has 175 billion neuron parameters. Thus, ChatGPT is no less intelligent than human beings. Because of the new human-computer interaction experience brought by this intelligence, ChatGPT has become the fastest popularized technology software in history with its user scale breaking 100 million after only two months of its launch. It is worth noting that the double-edged sword effect of technology should always be alerted to the fact that the development of any new technology is inseparable from the supervision and restraint of the supporting system: under the threshold of the legal system, the legal regulation issues behind this highly intelligent and rapidly popular technology must also receive the attention of the jurisprudence. From the perspective of criminal law, although ChatGPT and other generative AI have not yet caused major problems, the hidden criminal risks behind them cannot be ignored. In judicial practice, there have been cases of frauds committed by using generative AI: criminals use generative AI technology to disguise themselves as the victim's friends by changing their faces and voices so as to obtain money. In this regard, the criminal law should respond. In this article, we analyze the various criminal legal risks arising from the use and development of generative artificial intelligence such as ChatGPT, and propose measures to address them in order to achieve criminal compliance with the leapfrog development of generative artificial intelligence technology.[1]

2. Generative Artificial Intelligence After the Launch of ChatGPT

The approach to the study of legal phenomena under the perspective of legal philosophy cannot be separated from the categories of ontology, epistemology and methodology. The criminal risk and governance mechanism of ChatGPT and other generative AI belong to the epistemological and methodological spheres,[2] respectively, and therefore, before discussing these two spheres, a fundamental analysis of its ontology, i.e., ChatGPT and other generative AI, must be conducted.

2.1 The Conceptual Texture of Generative Artificial Intelligence and Its Historical Lineage

The original version of the concept of generative AI is "artificial intelligence-generated content", which refers to "a new type of production method that uses artificial intelligence technology to automatically generate new content", and this concept originated in 1950 when Alan Turing, who is regarded as the father of artificial intelligence and computers, proposed the famous concept of generative AI. Turing's famous "Turing test", which was used to determine whether machines were "intelligent", i.e., whether they could generate content and interact with humans in the same [3]way that humans think. In a way, the idea that AI could create content on its own was already created at that time.

The maturity of "AI-generated content" technology is often judged by comparing the degree of similarity between the generated content and similar human creations. After more than 60 years of precipitation and development, the technology formally entered the right track in 2014 with the introduction and iterative update of deep learning algorithms represented by "generative adversarial networks", and its generation methods and generators have become more and more intelligent and realistic, gradually reaching the point where human beings are difficult to distinguish, such as Microsoft's. For example, in 2017, Microsoft's artificial intelligence girl "Ice" created a poetry book *Sunshine Lost the Glass Window*, and in 2021, OpenAI released DALLE2, which can draw autonomously based on descriptors, marking the continuous growth of "artificial intelligence generated content" technology.[4]

With the launch of ChatGPT, "AI generated content" technology has come to a whole new stage, and the algorithm model behind it represents a major breakthrough in AI, and the concept of "generative AI" has officially emerged. According to Article 2 of the "Management Measures for Generative Artificial Intelligence Services (Draft)" issued by the State Internet Information Office in April 2023, generative AI refers to "technology that generates text, images, sound, video, code and other content based on algorithms, models and rules". From the concept, compared with the concept of "artificial intelligence generated content" in the expression of more standardized, marking the technology formally entered the vision of the legal system, a clear legal threshold in the positioning of "technology", for the subsequent legal norms laid the continuation of the creation of the foundation for the continuation of subsequent legal norms is laid.[5]

2.2 Operational Model and Technical Features of Generative AI in the Context of ChatGPT

As mentioned earlier, the introduction of ChatGPT has brought the generative AI technology into a new stage, and in fact other generative AI software such as Stable Diffusion and FaceSwap are currently developed based on the technical model of ChatGPT, according to which understanding the operation mode of ChatGPT can help us summarize the current generative Artificial intelligence technology features.

In terms of the underlying technical architecture, ChatGPT adopts an architecture of natural language processing and search engine integration, which gives it the ability of language understanding and text generation to complete the tasks of user instructions. In other words, the underlying logic of ChatGPT is essentially a linguistic big data model and a deep learning model: after converging an extremely wide range of language vocabularies, it is continuously anthropomorphized through a huge computing power in the process of learning and training time and again, thus exhibiting human-like traits. The operational logic of other generative AI is unparalleled, and thus characterized in terms of following traits: [6]

One of them is extremely high intelligence. The current generative AI has a very high intelligence, which is mainly reflected in the human-computer interaction experience, and is expressed through the authenticity of the generated objects. The current generative AI software is basically the same as real people in terms of interactivity: take ChatGPT and AI drawing technology as examples, users will feel like they are talking to real people in the process of using ChatGPT, which is a reflection of the authenticity of ChatGPT text products; the current AI drawing software can imitate and redraw any painting, as if a real person is a painter. This is the embodiment of the authenticity of AI drawing picture products. All of the above shows that the current generative AI has a high degree of intelligence.

Second, the dependence on big data. Generative AI relies on a huge data base, data is the core element of generative AI, its operation, development are dependent on the huge data support. For example, the current ChatGPT4 is a huge model with more than 100 trillion level parameters, which trains itself by continuously crawling the public data in the Internet and gets further developed in the process of training.[7]

Third, the breadth of applicability. The current generative AI technology has a very high universality, which is reflected in two aspects: first, the breadth of application, although the technology itself is still in the embryonic stage under the ChatGPT4 model, but from the trend of application scope popularity, it has gradually started to form a large-scale application covering most of the global industries; on the other hand, the generative AI technology under the new algorithm model. On the other hand, the generative AI technology under the new algorithm model has a strong self-learning capability, which almost does not require human intervention in the application process of specific software, thus greatly reducing the threshold of using the technology and expanding the number of users exponentially.[8]

In summary, the current generative AI technology refers to the technology that generates text, images, sounds, videos, codes, and other contents based on algorithms, models, and rules, and is characterized by high intelligence, big data dependency, and wide applicability. The analysis of risks and the discussion of governance measures below all revolve around this basic concept and feature.

3. Criminal Legal Risk Analysis of Generative Artificial Intelligence Represented by ChatGPT

(1) Response to the Need for Criminal Risk Research

At present, research on generative AI such as ChatGPT is mainly focused on the civil field, and little mention has been made of its criminal risks. In fact, some scholars have taken a negative attitude toward the study of the criminal risks of AI, arguing that the development of AI is actively tackled and regulated by criminal law, which is "a phantom put together by countless imaginations, scaring oneself with other people's 'gimmicks'". The author believes that the study of the criminal risk of artificial intelligence, especially the current criminal risk of generative artificial intelligence is not an empty talk, nor is it a hypothetical problem, but based on the current practice of the objective development of artificial intelligence technology, the response and avoidance of the criminal risk that has come or will come, which is determined on the basis of the relevance of the infringement of criminal law interests. For example, back in 2019, criminals began using AI-generated content technology to imitate the voice of an executive of that energy company, whose executive director followed instructions to make a transfer after receiving [9]a call from that voice, losing up to $240,000. ChatGPT had not yet been launched, and the generative AI technology was not yet mature enough for employment to be such a criminal risk, and how could it be a "phantom" to explore the criminal risks of generative AI in the context of the technology?[10]

In fact, the current development of generative artificial intelligence technology, its social harm also expanded at the same time, the use of the technology to commit crimes intensified: at present, the term "AI fraud" has formed a certain degree of heat in the country, the police emergency issued the new fraud prevention guide; through face replacement technology to create yellow rumors, the dissemination of obscene material is also further widespread. The spread of obscene material has also become more common. All of the above criminal risks already exist, revealing the need to study the criminal risks of generative AI; from the perspective of the technology's development prospects, the potential risks of generative AI should not be underestimated, such as big data security risks, risks of bad generators and other security issues that must be taken seriously in the era of network information.[11]

Accordingly, the issue of criminal risk of generative AI technology is not a castle in the air, and the study of the issue is based on social practice using the legal system to adjust social practice, forming the system and technology, law and social coordination of the rightful meaning.

(2) Specific Criminal Risk Types Under the Perspective of Legal Benefit Aggressiveness

Based on the concept of generative AI and its technical characteristics, we can summarize the types of criminal law risks involved in generative AI in the light of the specific legal interests protected by criminal law norms:

3.1 Data Security Risks in the Use of Generative AI Technology Using ChatGPT as an Example

As mentioned above, generative AI technology is highly dependent on big data, and its learning, training and even the operation of the various aspects of result generation are inseparable from the support of data. Take ChatGPT as an example, as explained in the previous section, ChatGPT4 currently has a database of trillions of data, and its database is still expanding as users continue to input all kinds of data, including sensitive data, into it during use. This reveals a concern that cannot be ignored: the data security of all the data contained in the database. Although OpenAI promises users that it will protect their conversations with ChatGPT, no technology is perfect, and there are always vulnerabilities that can be exploited by criminals for criminal purposes. While this may seem like a technical issue, from a criminal law perspective, the risk of data security violations embodied in the operation of ChatGPT is inherently present, in the following ways:

First, the legality of the source in the process of data collection and development. From ChatGPT1 to the current ChatGPT4, the number of model parameters behind it has grown exponentially in the iterative process, and the database has jumped from 117 million to 100 trillion, reflecting its ability to collect massive amounts of Internet data, and from the source of the collected information database, OpenAI has not announced the data sources used, and whether the relevant data sources are authorized. At the same time, since ChatGPT requires little human intervention in the process of use, this means that ChatGPT is also free from human intervention and control in acquiring data, according to which the legality of [12]the data source is not controllable. For example, users who create illegal websites or upload pirated e-books or even illegal information on websites can also become their learning data. Accordingly, the data collection R&D of models such as ChatGPT possesses criminal risks.[13]

Second, Data leakage problem. Under the situation of widespread application of information technology and rapid development of big data industry, "technical leviathan" cannot be avoided, and data leakage itself is a persistent problem of data security in the Internet information era, which is mainly manifested as three kinds of problems in ChatGPT: suspected leakage of user privacy and personal information data, which is suspected of infringement of citizens' personal information; leakage of commercial secrets, which constitutes a crime of infringement of personal information, etc. The leakage[14] of commercial secrets, which constitutes unfair competition and endangers the normal operation of commercial companies, is suspected of infringement and illegal provision of commercial secrets; the leakage of state secrets, which may constitute a danger to national security, is suspected of illegal acquisition and illegal provision of state secrets.

3.2 The Multiple Risks of Generative AI Technology Generators

Based on the concept of generative AI, its generators mainly include text, images, sound, video, code and other contents. Our pursuit of the technical products of generative AI is often "real and close to the real product". Therefore, according to the "high intelligence" characteristics of the current generative AI, its products are often highly realistic and difficult to be distinguished by the general audience, thus generating multiple criminal risks:

The first is in the area of intellectual property legal interests. Since the underlying technical logic of generative AI is to learn and train to achieve the fidelity of the generator, if the learning data is limited to a specific work, it can be trained to be infinitely close to that specific work, as internationally renowned linguist Chomsky said: "ChatGPT is a high-tech plagiarism system" that discovers patterns from massive amounts of data, and then follows the rules to make the data more realistic. The use of generative artificial intelligence to generate a highly similar product to another's work and to reproduce and sell it for profit is suspected to constitute the crime of copyright infringement and the crime of selling infringing copies.[15]

The second is in the area of citizens' personal and property rights. The deep synthesis technology developed by generative artificial intelligence technology, also known as deep forgery, namely "artificial intelligence algorithms in neural network recognition and audition data generation and transformation processing technology", commonly known as AI face replacement, AI synthetic voice technology. This technology has become a new type of fraudulent means for criminals, for example,[16] the perpetrator generates the portrait, voice and other characteristics of people familiar to the victim through the technology to impersonate others for fraud, due to the high fidelity of the generated objects the victim is often difficult to distinguish and thus falls for the fraud, and receives damage to property rights. In addition, the use of depth synthesis technology to replace another person's face into the pornographic video[17] and spread, involves the infringement of the reputation of others, suspected of constituting insult, defamation.

Finally, in terms of national security and social order. Generative artificial intelligence technology may also raise the risk of national security and social order. For example, if a false video is created through deep synthesis technology to incite national hatred and harm national unity, or if false terrorist information or disaster information is created to cause serious social order disturbance, or if pornographic, obscene audio, video, or picture information is created using related technology for large scale dissemination... such acts are within the scope of criminal regulation. Such criminal risks should also be addressed.

4. Challenges in the Governance of Criminal Risks of Generative Artificial Intelligence in the Context of ChatGPT

The criminal risks posed by generative AI challenge our current criminal policies and legal norms to address them. Its powerful technological capabilities have inevitably impacted the relatively stable criminal legal system by changing the trend of productivity and production relations; the traditional mechanism of responsibility allocation centered on the system of rights and obligations is gradually deconstructed under the influence of the developed digital technological capabilities. The criminal risk governance of generative AI is in fact faced with the double test of traditional criminal law theory and criminal law norms.

(1) Doubts of the Main Attribution System

According to the general theory, the position of AI in the criminal subject can be divided into "weak AI" and "strong AI", weak AI is essentially a tool technology and cannot become a criminal subject; strong AI can become a criminal subject because it has the ability to control and identify. The strong AI can become a criminal subject because it has the ability to control and identify. It is generally believed that the current AI technology still belongs to weak AI, thus, generative AI such as ChatGPT is still a technical tool and does not have the status of a criminal subject itself and is not imputable. However, the reality is that crimes committed with the participation of generative AI such as ChatGPT have gradually torn apart the traditional imputation system and the basic principle of adaptation of crime to punishment.[18][19]

According to the traditional criminal attribution system, the use of generative AI, such as ChatGPT, to commit crimes is essentially no different from traditional crimes in that the person who uses it has the power over the criminal act and result is criminally responsible for the consequences, and the AI exists as a "tool" in it. However, in fact, there are loopholes in this instrumentalist view on the attribution of responsibility for the generated material: the current generative AI technologies such as ChatGPT predict the outcome by imitating the mode of operation of human neural networks, and the generated content is not predictable for the program developers and program users, and its generation process page completely excludes human[20] intervention. According to the viewpoint of "instrumentalism", only the user is responsible for the uncontrollable generation mode, which in fact violates the principle of compatibility between crime and punishment, and logically does not make sense.[21]

We can imagine a specific scenario where a user uploads a photo of himself and his girlfriend on the beach to ChatGPT, and then the photo is widely disseminated because his girlfriend is wearing a cool dress and is outputted by other users with the label "porn star". According to the traditional criminal imputation theory, the user's behavior was not harmful and therefore not liable, but in fact the woman's reputation was actually harmed. Thus, the traditional criminal subject attribution system is not sufficient to deal with the criminal risk management of generative AI.

(2) Inadequacy of the Crime Regulation System

It is difficult to effectively manage the criminal risks posed by generative AI such as ChatGPT under the current criminal law regime. This stems from two main elements:

First, the modesty principle of criminal law has resulted in an ex post facto mode of regulation in the crime system of criminal law sub-clauses, for example, the crimes of insult, defamation, fraud, etc. in respect of citizens' personal property, or the crimes of secession, incitement to secession, and dissemination of obscene materials in respect of national and social security are regulated from an ex post facto perspective, i.e., the acts are regulated after the birth of harmful consequences. The crime is regulated only after the harmful consequences have been created. From the perspective of using ChatGPT and other generative artificial intelligence crimes, on the one hand, the difficulty and cost of using this technology is extremely low, and can be hidden from detection through layers of network technology; on the other hand, it is often difficult to recover from the harmful results formed by the harmful acts, which is commonly known as "a mouthful of rumors, disinformation runs out of legs". Therefore, the ex post facto model of regulation is inadequate in dealing with the risks posed by generative artificial intelligence technologies such as ChatGPT.[22]

Second, the current criminal legal norms do not match the needs of technological development. Taking data crimes in China's criminal law as an example, the crime system formed by China's criminal law on data security protection focuses on the illegal acquisition of data, highlighting a static protection of China's data security focusing on the formation of a stable and exclusive control state of data by the right holder, while in the era of generative AI, the value of data is in its mobility, ChatGPT and other generative AI, such as ChatGPT, captures data through data collection, analyzes and learns the data, and outputs it to form new data, and then repeats[23] the process on top of the new data to achieve self-correction. As a result, the development needs of technology and the protection concept of legal norms are in conflict, which leads to the risk management inevitably caught in a back-and-forth trade-off between technological development and protection of legal interests, lacking in normality and hindering the concept of fairness and justice of law.[24]

5. The Construction of Criminal Risk Governance Path

The criminal risks posed by generative AI technologies reveal the urgency of criminal law intervention, while the current governance challenges indicate that the intervention of criminal law cannot be too direct, its regulatory process is not straightforward, and the governance concept needs to be adjusted urgently. The author believes that, first of all, the object of regulation should be clarified, and on the basis of the basic object of regulation, the criminal risk governance should be achieved through the construction of a pluralistic subject responsibility allocation mechanism and a hybrid criminal-civil law regulatory framework system.

(1) Data as the Core Object of Regulation

According to the above, the operation process of generative artificial intelligence is reflected in the collection, learning and generation of data, and without data, it loses its foundation of existence. Therefore, data should also be the fundamental object of regulation in the governance path, specifically:

First, the data collection behavior of generative AI should be regulated. Generative AI should not collect all information and data without restriction, and should establish a hierarchical management system based on the sensitivity and confidentiality of data. For government core data, personal privacy, and commercial secrets, the collection and use of generative AI should be restricted, while other types of information should be subject to different degrees of restrictive requirements, such as the authorized use of personal information data.[25]

Secondly, the idea of data regulation is changed to focus on the regulation of data misuse. The criminal risk of generative AI technology mainly comes from the act of using the technology to commit crimes, and the key manifestation is the act of data misuse. The current criminal law focuses on the unlawful acquisition of data or helping individuals to possess data, and lacks regulation of data misuse, so relevant judicial interpretations or legal provisions should be added to focus on regulating data misuse.[26]

Third, barriers should be set up at the technical level and algorithmic logic to prevent data leakage. From the technical level, the developers of generative AI should continuously strengthen information protection and put a lock on the layers of information collected by the technology in the process of use to prevent unlawful elements from illegally obtaining relevant information; from the algorithmic logic, the morality of generative AI should be enhanced, such as refusing the generation of content involving information that leaks personal privacy, commercial secrets, state secrets, etc.

(2) Establishing a System for Assigning Responsibility to Multiple Subjects

The current generative AI does not have the status of a criminal subject, so it cannot be criminally responsible, which is an unchangeable premise under the current criminal law system. As mentioned in the previous article, the way of attribution from the user's perspective is not sufficient to deal with the existing criminal risks, and inevitably there is no attribution. Therefore, the management of technical criminal risks should build a mechanism to allocate the responsibility of multiple subjects. Specifically:

Increase the compliance responsibility of developers. Generative AI technology developers should take the initiative to fulfill their technical safety and compliance obligations, which comes from their natural technical and information advantages. On the one hand, the developer should be obliged to protect the user's input information and usage records in the process of providing services; on the other hand, the developer should optimize the algorithm model to eliminate the generation of undesirable contents, and at the same time, establish a corresponding relief mechanism to take remedial measures when users report the infringement of the generated products.[27]

Increase the censorship responsibility of platforms. Therefore, online social media should review the content posted on the platform, and such review should be conducted in two aspects: first, the labeling behavior of the platform, if it involves generative AI technology, it should be labeled in a conspicuous way to inform other users; and second, the labeling behavior of the platform. The second is the user's declaration behavior, the platform should also require users to upload generative AI products should take the initiative to explain the situation, and to discipline the offending users.

Increase the supervision responsibility of public authorities and institutions. With the wave of technology, public institutions, as the "public interest advocates", should play their role as the "helmsman" and actively perform their supervisory responsibilities to ensure that the technology runs in the right track. Specifically, firstly, they should promote the process of establishing and improving corresponding laws and regulations to ensure that there is a law to follow in the process of supervision; secondly, they should implement law enforcement and supervise the application of the law, including supervising whether developers have implemented their own compliance responsibilities, whether social media platforms have fulfilled their censorship responsibilities, and whether users have violated the application of technology, and punishing each subject for violating laws and regulations.

If the above-mentioned subjects fail to properly perform their duties, resulting in serious consequences, they should be held civilly and administratively liable in strict accordance with the liability allocation mechanism under the principle of dominance, according to "whoever is responsible for the risk and the consequences arising from it falls within the jurisdiction", and criminal liability should be investigated in accordance with the law if it constitutes a crime.[28]

(3) Construction of a Mixed Legal Normative Framework for Criminal and Civil Acts

The legal regulation of innovative technologies is an eternal challenge, especially in criminal legal norms, because criminal law has strong disciplinary attributes, the wind direction of its modification will also largely affect the development of technology, too deep intervention hinders the development of technology, too shallow intervention leads to technology abuse. The construction of the legal regulatory framework of generative AI requires a change in the thinking of criminal regulation on the one hand, and the adjustment role of civil law and administrative law on the other hand to carry out.

First of all, in the criminal field, we should pay attention to the development needs of generative AI technology and avoid the excessive intervention of strong disciplinary criminal law norms. Some scholars advocate that "in order to screen and prevent risks while protecting the enthusiasm and creativity of artificial intelligence research and development, it is necessary to take more soft law approach, rather than simply improve the hard law of discipline", I agree with this. From the legislative practice of various countries, including China, the legal norms for generative AI technologies are focused on guidance of behavior rather than punishment. For example, the European Commission issued the "Uniform Rules on the Development of Artificial Intelligence", the United States issued the "Artificial Intelligence Risk Management Framework", including the aforementioned laws and regulations in China, the core purpose is to guide different subjects to take measures to establish risk prevention mechanisms, rarely involving the prohibition of behavior and disciplinary provisions.[29]

Second, the role of governance in the civil and administrative fields should be highlighted. This is, on the one hand, because the conservative model of criminal intervention orientation implies the need to pay more attention to the role of norms in the civil and administrative spheres in order to achieve a dynamic balance of the legal normative governance framework, and, on the other hand, because the risk management of generative AI technologies such as ChatGPT relies on the establishment of an ex ante prevention model, while the regulation model of criminal law is an ex post regulation model, which is in the construction of ex ante prevention. In the field of civil law, it is important to consider the following. Therefore, in the field of civil law, the relevant legal provisions should be further updated in the light of the generative AI technology, for example, by responding to the copyright infringement of generative AI works to prevent further criminal risks of intellectual property rights, or by strengthening the personal information protection mechanism, by expanding the scope of personal information, the types of illegal use of personal information to prevent further criminal risks to citizens' personal and property. In the field of administrative law, law enforcement should be carried out in strict accordance with the administrative regulations related to network security and the newly introduced "in-depth technology management regulations", and promote the completion and implementation of the specific specifications of the "Generative Artificial Intelligence Service Management Measures (Draft for Comments)", aiming to build a comprehensive technical compliance mechanism jointly constructed by the government, enterprises and citizens at the social level.

6. Conclusion

The technical prospect brought by the generative AI technology in the context of ChatGPT undoubtedly makes all levels of society full of, and inevitably anxious about, its risks. It is undeniable that, as the engine of a new technological revolution, the torrent of the era triggered by AI technology is still irresistible, and what is open to the legal community is the surging demand for technological development, on the one hand, and the iterative risks that cannot be ignored on the other. Throughout the emergence of each new technology, it is accompanied by a long-term normative process, and the harmonious relationship between technology and norms needs to be explored over a long period of time and constantly revised in order to reach a balance. The position of this paper is that in the face of the criminal risks arising from generative AI technologies such as ChatGPT, its governance should follow a process from loosening to tightening, and a certain degree of freedom should be given to the development of the technology during its infancy when its future is still unclear. In terms of criminal law regulation, on the one hand, it is necessary to maintain the principle of modesty and avoid the overstepping of criminal law on the basis of establishing a sound civil protection mechanism; on the other hand, it is necessary to appropriately adjust part of the crime system, especially in data crimes, in order to meet the development trend and needs of technology.

References

Deng Jianpeng and Zhu Bonnie Cheng. (2023). "Legal Risks of ChatGPT Models and Countermeasures", in *Journal of Xinjiang Normal University*, (5), p. 94.

Ji Weidong. (2019). "The Concept, Law, and Policy of Artificial Intelligence Development," in *Eastern Jurisprudence*, (5).

Jianpeng Deng and Bonnie Cheng Zhu. (2023). "Legal Risks of ChatGPT Models and Countermeasures", in *Journal of Xinjiang Normal University*, (5), p. 91.

Lao Dongyan. (2018). "Rethinking and Reconstructing the Theory of Foreseeability in Negligence", in *Chinese and Foreign Law, 2*(2), p. 319.

Laodongyan. (2020). "The Criminal Law Protection Model of Personal Data", in *Comparative Law Research*, (5), p. 42.

Li Buyun. (2009). "An Outline of the System and Basic Categories of Philosophy of Law", in *Modern Jurisprudence, 1*(1), p. 3.

Li Zhenlin, Pan Xinyuan. (2023). "The Dilemma of Criminal Law Protection of Data Security in the Context of Generative Artificial Intelligence and Response to the Development of ChatGPT as a Perspective," in *Crime Research*, (2), p. 30.

Liu Xianquan. (2018). "Internal Problems, External Problems and Criminal Liability in the Era of Artificial Intelligence," in *Eastern Law, 1*(1), p. 134.

Liu Yanhong. (2019). "The Anti-intellectualization Critique of Artificial Intelligence Jurisprudence Research", in *Eastern Law, 5*, p. 122.

Shu Hong and Peng Peng. (2023). "Legal Risks and Countermeasures of Disinformation in ChatGPT Scenarios," in *Journal of Xinjiang Normal University, 5*(5), p. 127.

Wang Yang and Yan Hai. (2023). "Risk Iteration and Regulation Update of Generative AI with ChatGPT as an Example", in *Theory Monthly*, (6), p. 21.

Xiong Bo. (2020). "The Risk of Expanding Criminal Governance and the Limits of 'Deep Forgery'", in *Journal of Anhui University, 6*, p. 106.

Xiong Qi. (2017). "The Copyright Determination of Artificial Intelligence Generated Objects," in *Intellectual Property, 3*(3), p. 7.

Xu Xin and Liu Weichao. (2023). "Cold Thinking in the ChatGPT Boom: Be Wary of Information Tools Used for Cognitive Confrontation," in *Studies in Culture and the Arts, 1*(1), p. 74.

Yao Wanqin. (2019). "Questioning the Risk of Artificial Intelligence through New Crimes," in *Contemporary Law, 3*(3), p. 13.

Yu Changzhi. (2022). "From Control to Utilization: A Paradigm Shift in Criminal Law Data Governance," in *Chinese Social Sciences*, (7), p. 58.

Yuan Zeng. (2023). "Study on the Liability of Generative Artificial Intelligence," in *Oriental Law, 3*(2023), p. 19.

Yuan Zeng. (2023). "Study on the Liability of Generative Artificial Intelligence", in *Oriental Law, 3*(3), p. 20.

Zhang Xu. (2022). "Research on Criminal Governance of Crimes against Citizens' Personal Information", in *Journal of Social Sciences of Jilin University*, (6), p. 62.

Zhu Guanghui, Wang Xiwen. (2023). "ChatGPT's Operation Model, Key Technologies and Future Approaches" in *Journal of Xinjiang Normal University, 4*(2023), p. 120.

[1] See WeChat: Company owner cheated 4.3 million! AI fraud is breaking out across the country! Please keep these fraud prevention points in mind. https://mp.weixin.qq.com/s/7uY3bcqD6Kvx1CmiwFjPGg, 2023.5.23.

[2] See Li Buyun. (2009). "An Outline of the System and Basic Categories of Philosophy of Law", in *Modern Jurisprudence, 1*(1), p. 3.

[3] See China Communications Academy: "AI-Generated Content White Paper (2022)", http://www.caict.ac.cn/sytj/202209/P020220913580752910299.pdf, 2023.5.23.

[4] Generative adversarial networks are deep learning models that provide artificial intelligence to learn in

unsupervised learning mode and enrich its own database, and are the core underlying technology of generative AI technology.

[5] See State Internet Information Office: "Generative Artificial Intelligence Services Management Measures (Draft for Comments)" http://www.cac.gov.cn/202304/11/c_1682854275475410.htm, 2023.5.23.

[6] See Jianpeng Deng and Bonnie Cheng Zhu. (2023). "Legal Risks of ChatGPT Models and Countermeasures", in *Journal of Xinjiang Normal University*, (5), p. 91.

[7] See Zhu Guanghui, Wang Xiwen. (2023). "ChatGPT's Operation Model, Key Technologies and Future Approaches" in *Journal of Xinjiang Normal University, 4*(2023), p. 120.

[8] See Yuan Zeng. (2023). "Study on the Liability of Generative Artificial Intelligence," in *Oriental Law, 3*(2023), p. 19.

[9] Liu Yanhong. (2019). "The Anti-intellectualization Critique of Artificial Intelligence Jurisprudence Research", in *Eastern Law, 5*, p. 122.

[10] Relying on the boss's voice to cheat away 1.82 million! Audio version of Deepfake makes employees transfer money obediently, https://baijiahao.baidu.com/s?id=1673801021443841142&wfr=spider&for=pc, 2023.5.23.

[11] "AI fraud is breaking out across the country", the police urgently reminded, https://new.qq.com/rain/a/20230524A01VL800, 2023.5.23.

[12] See Xu Xin and Liu Weichao. (2023). "Cold Thinking in the ChatGPT Boom: Be Wary of Information Tools Used for Cognitive Confrontation," in *Studies in Culture and the Arts, 1*(1), p. 74.

[13] See Deng Jianpeng and Zhu Bonnie Cheng. (2023). "Legal Risks of ChatGPT Models and Countermeasures", in *Journal of Xinjiang Normal University*, (5), p. 94.

[14] See Zhang Xu. (2022). "Research on Criminal Governance of Crimes against Citizens' Personal Information", in *Journal of Social Sciences of Jilin University*, (6), p. 62.

[15] Noam Chomsky: The false promise of ChatGPT, New York Times, 202338.

[16] According to the "Internet information service depth synthesis management regulations", depth synthesis technology refers to the deep learning, virtual reality as the representative of the generation of synthesis class algorithm to produce text, images, audio, video, virtual scenes and other information technology, belongs to a generative artificial intelligence technology.

[17] Xiong Bo. (2020). "The Risk of Expanding Criminal Governance and the Limits of 'Deep Forgery'", in *Journal of Anhui University, 6*, p. 106.

[18] See Liu Xianquan. (2018). "Internal Problems, External Problems and Criminal Liability in the Era of Artificial Intelligence," in *Eastern Law, 1*(1), p. 134.

[19] Yuan Zeng. (2023). "Study on the Liability of Generative Artificial Intelligence", in *Oriental Law, 3*(3), p. 20.

[20] See Yao Wanqin. (2019). "Questioning the Risk of Artificial Intelligence through New Crimes," in *Contemporary Law, 3*(3), p. 13.

[21] See Xiong Qi. (2017). "The Copyright Determination of Artificial Intelligence Generated Objects," in *Intellectual Property, 3*(3), p. 7.

[22] See Shu Hong and Peng Peng. (2023). "Legal Risks and Countermeasures of Disinformation in ChatGPT Scenarios," in *Journal of Xinjiang Normal University, 5*(5), p. 127.

[23] See Yu Changzhi. (2022). "From Control to Utilization: A Paradigm Shift in Criminal Law Data Governance," in *Chinese Social Sciences*, (7), p. 58.

[24] See Li Zhenlin, Pan Xinyuan. (2023). "The Dilemma of Criminal Law Protection of Data Security in the Context of Generative Artificial Intelligence and Response to the Development of ChatGPT as a Perspective," in *Crime Research*, (2), p. 30.

[25] Wang Yang and Yan Hai. (2023). "Risk Iteration and Regulation Update of Generative AI with ChatGPT as an Example", in *Theory Monthly*, (6), p. 21.

[26] See Laodongyan. (2020). "The Criminal Law Protection Model of Personal Data", in *Comparative Law Research*, (5), p. 42.

[27] See "Measures for the Administration of Generative Artificial Intelligence Services (Draft for Comments)," http://www.cac.gov.cn/202304/11/c_1682854275475410.htm, 2023.5.26.

[28] Lao Dongyan. (2018). "Rethinking and Reconstructing the Theory of Foreseeability in Negligence", in *Chinese and Foreign Law, 2*(2), p. 319.

[29] See Ji Weidong. (2019). "The Concept, Law, and Policy of Artificial Intelligence Development," in *Eastern Jurisprudence*, (5).